KDM Analytics™

OBJECT MANAGEMENT GROUP

# *System Assurance Approach with Focus on Automation*


**Djenana Campara**

CEO, KDM Analytics

Board Director, Object Management Group (OMG)

Co-Chair System Assurance and Architecture Driven Modernization TF, OMG

# *Who Is OMG?*

**Object Management Group (OMG) factoids:**

- Founded in 1989
- Over 470 member companies
- The largest and longest standing not-for-profit, open-membership consortium which develops and maintains computer industry specifications.
- Continuously evolving to remain current while retaining a position of thought leadership.

# *OMG's Best-Known Successes*


**Common Object Request Broker Architecture**

- CORBA® remains the only language- and platform-neutral interoperability standard

**Unified Modeling Language**

- UML™ remains the world's only standardized modeling language

**Business Process Modeling Notation**

- BPMN™ provides businesses with the capability of understanding their internal business procedures

**Common Warehouse Metamodel**

- CWM™, the integration of the last two data warehousing initiatives

**Meta-Object Facility**

- MOF™, the repository standard

**XML Metadata Interchange**

- XMI™, the XML-UML standard

# *Who Are OMG-ers?*

Some of the hundreds of member companies;

| | | | |
|---|---|---|---|
| **ACORD** | **Deloitte** | **Mega Practical** | **Progress** |
| **Atego** | **Fujitsu** | **MetaStorm** | **Red Hat** |
| **BAE Systems** | **General Dynamics** | **Microsoft** | **SAP** |
| **Boeing** | **HP/EDS** | **Navy UWC & SWC** | **Selex** |
| **CA** | **Harris** | **NEC Sphere** | **Software AG** |
| **Capgemini** | **Hitachi** | **Northrop Grumman** | **Sopra** |
| **Cordys** | **HSBC** | **No Magic** | **Sparx Systems** |
| **CSC** | **IBM** | **Oracle** | **Tata** |
| **DND Canada** | **KDM Analytics** | **Penn National** | **Tibco** |
| **FICO** | **Lockheed Martin** | **PrismTech** | **Vangent** |

# *Liaison Relationships*








# OMG Organization

## Architecture Board

Liaison SC
Object & Reference Model SC
Spec Mgt SC
MDA Users' SIG
Process Metamodels SIG
SOA SIG
IPR SC
Sustainability SIG
Architecture Ecosystems SIG
Business Architecture SIG

## Platform TC

A & D PTF
ADM PTF
MARS PTF
SysA PTF
Agent PSIG
Data Distribution PSIG
Japan PSIG
Korea PSIG
Ontology PSIG
Telecoms PSIG

## Domain TC

BMI DTF
C4I DTF
Finance DTF
Government DTF
Healthcare DTF
Life Sciences DTF
Mfg Tech & Ind. Systems DTF
Robotics DTF
S/W Based Comm DTF
Space DTF
Crisis Mgmt DSIG
Regulatory Compl. DSIG
SDO DSIG
Sys Eng DSIG

## Community of Practice

SOA Consortium

Consortium for IT Software Quality (CISQ)

Cybersecurity Forum

# *OMG System Assurance Task Force (SysA TF)*

Claude Langton: But I haven't heard anything about a murder.
Hercule Poirot: No, you would not have heard of it. Because, as yet, it has not taken place. You see, if one can investigate a murder before it happens, then one might even, well, a little idea... prevent it?

Agatha Christie, Poirot: The Wasp's Nest.

- Strategy
  - establish a common framework for analysis and exchange of information related to system assurance and trustworthiness.
    - This trustworthiness will assist in facilitating systems that better support Security, Safety, Software and Information Assurance

- Immediate focus of SysA TF is to complete work related to
  - SwA Ecosystem - **common framework for presenting and analyzing properties of system trustworthiness**
    - leverages and connects existing OMG specifications and identifies new specifications that need to be develop to complete framework
    - provides integrated tooling environment for different tool types
    - architected to improve software system analysis and achieve higher automation of risk analysis

# *SwA Ecosystem: Reaching Beyond Vulnerability Detection*

- Conclusion that system is vulnerable can be based on the fact that at least one exploitable vulnerability is detected
- Opposite is not true - If no vulnerability is detected it still does not mean that system is secure!
- Different domains of knowledge contributes to “security posture of the software system” and needs to be considered during system assessments
  - Detailed knowledge of system
  - Knowledge of risks and threats to the system
  - Knowledge of system’s security requirements and safeguards
  - Knowledge of vulnerabilities
  - … and list goes on
  - cross-domain view knowledge created by integrating different domains of knowledge into assuring argument supported by evidence to answer “why system can be trusted”

**Integrated cross-domain knowledge into assuring argument supported by high fidelity fact-based evidence to the testimony of system’s security posture is possible only through standards**

# *Software Assurance (SwA) Ecosystem – Standard-based Solution*

- Standard-based integrated tooling environment that dramatically reduces the cost of multi-disciplinary software assurance activities

- Based on integrated ISO/OMG Open Standards
  - Semantics of Business Vocabulary and Rules (SBVR)
    - For formally capturing knowledge about vulnerabilities
  - Knowledge Discovery Metamodel (KDM)
    - Achieving system transparency in unified way
  - Structured Assurance Case Metamodel
    - Argumentation Metamodel (ARM) and Software Assurance Evidence Metamodel (SAEM)
    - Intended for presenting Assurance Case and providing end-to-end traceability: requirement-to-artifact
  - Structure Metrics Metamodel
    - Representing libraries of system and assurance metrics

## *Improving System Assessments*

Key Deliverables of SwA Ecosystem –

1. End-to-end Traceability: *from code to models to evidence to arguments to security requirements to policy*
2. Specified assurance compliance points through formal specification
3. Transparency of software process & systems
4. Standards based Integrated tooling environment

**Together, these requirements enable the management of system knowledge and knowledge about properties, providing a high degree of transparency, traceability and automation**

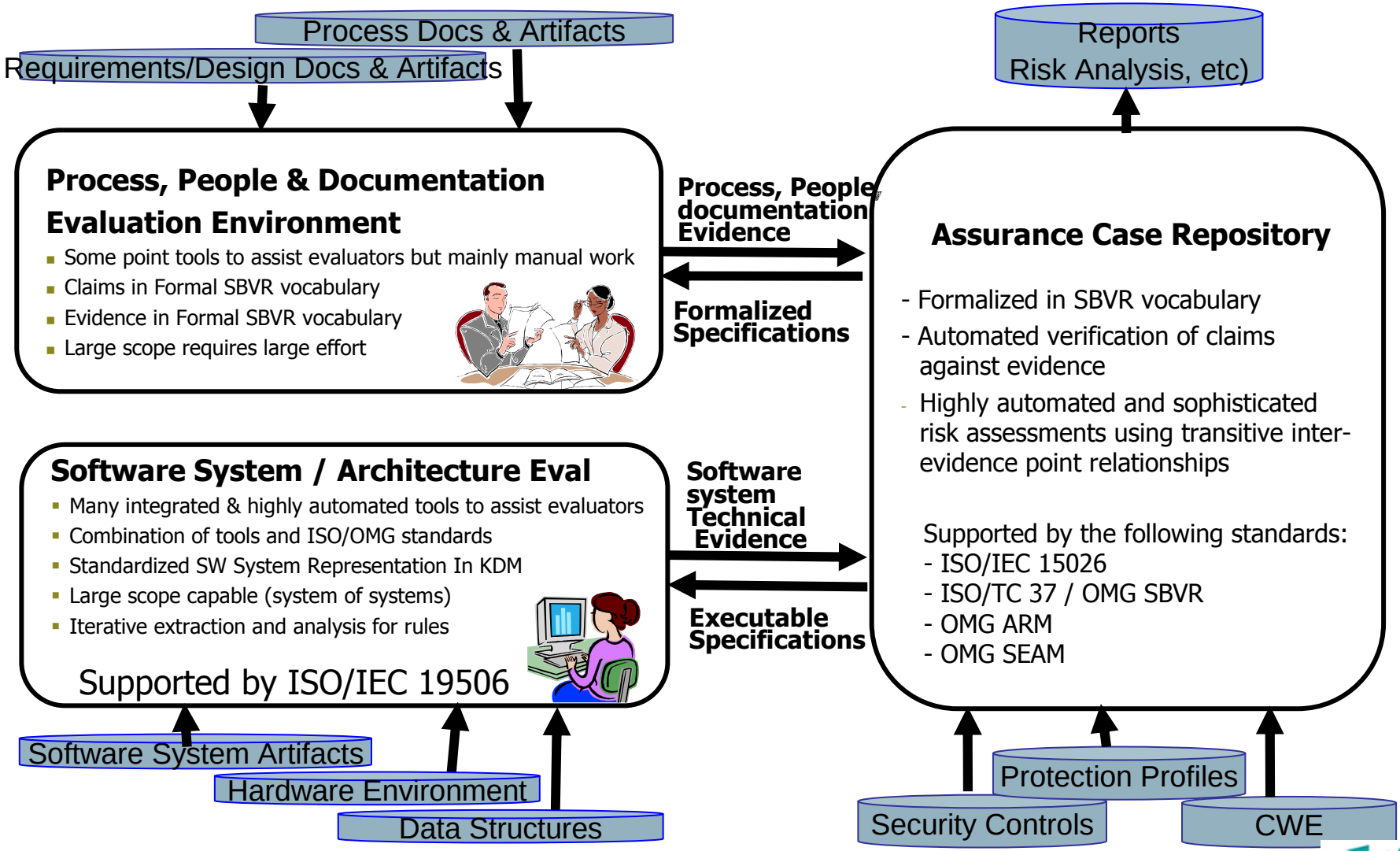
# *Software Assurance (SwA) Ecosystem – Going Forward*

- Work in the following areas
  - Risk Assessment Metamodel
  - Software Patterns Metamodel
  - Libraries of Software Fault Patterns
  - Libraries of Security Metrics
  - Defining Security Vocabulary

# *Software Assurance Ecosystem =*

*System Assurance Approach with Focus on Automation*

***Tools Interoperability and Unified Reporting Environment***

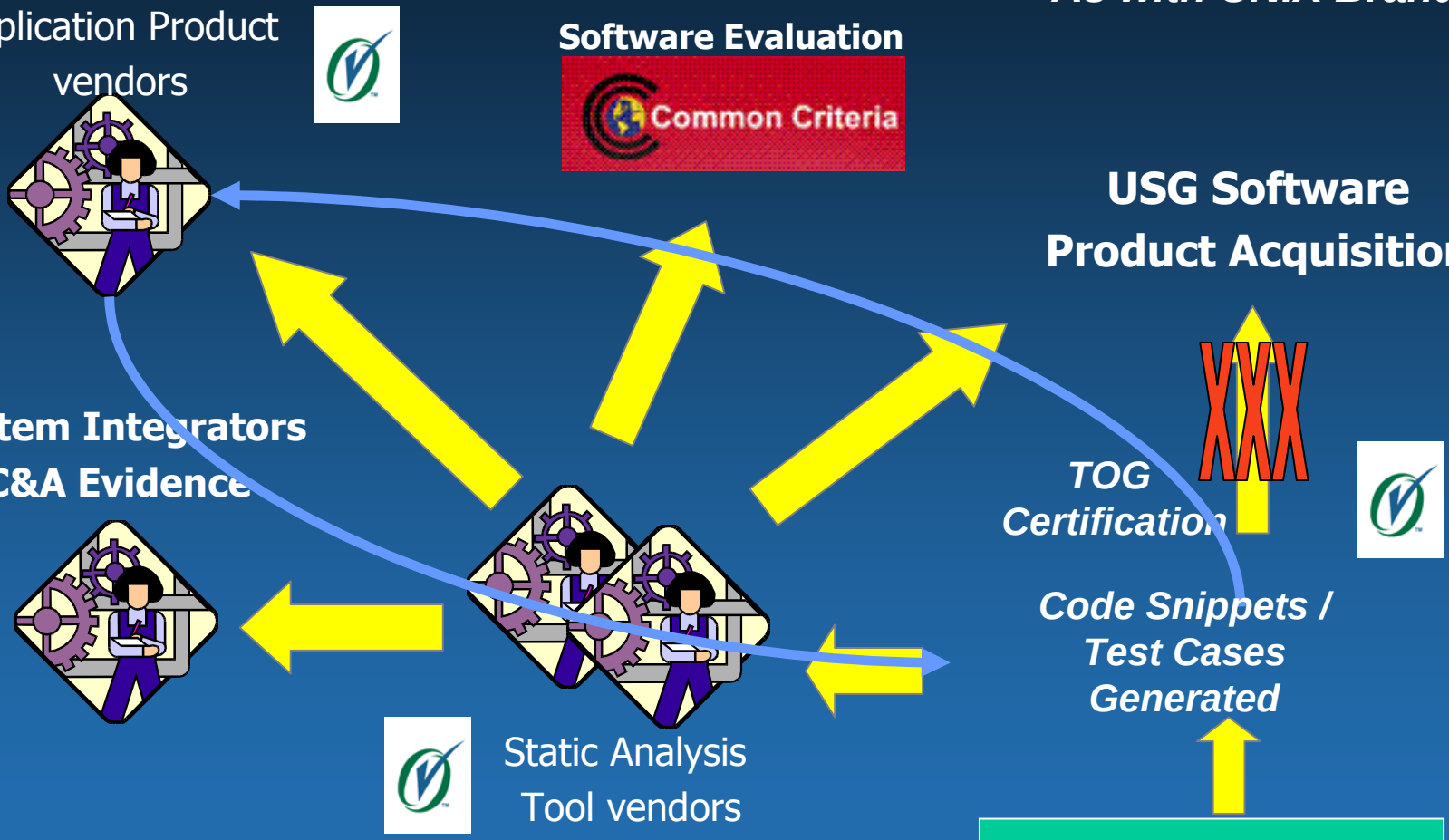



KDM Analytics ™

OMG OBJECT MANAGEMENT GROUP

# Ecosystem in Standards Process and Tool Certification

*As with UNIX Branding*




Prepared by Dr. Ben Calloni, LM Aero

# *Web Sites to Visit*

- http://www.omg.org
- http://sysa.omg.org
- http://kdmanalytics/swa
- http://www.omg.org/technology/kdm/index.htm - OMG published Knowledge Discovery Metamodel
- http://www.iso.org/iso/catalogue_detail.htm?csnumber=32625 – ISO published Knowledge Discovery Metamodel